Security report for the period October 2022- October 2024

Ofcom's 1st security report to DSIT Secretary of State in accordance with section 105Z of Communications Act 2003

Report

22 November 2024

Contents

Section

Overview

The Telecommunications (Security) Act 2021 was introduced following the previous Government's Telecoms Supply Chain Review and sought to establish *"a new security framework within which the Government sets out what good security looks like with a new security obligation on operators to raise the height of the security bar"*[1]. Ofcom was tasked with the role of monitoring and enforcing compliance with the framework.

The legislation was established to respond to serious threats that continue to be present today. The services and networks provided by the telecoms sector are an essential input to the rest of the UK's Critical National Infrastructure as well as directly underpinning many other economic and societal activities. At the same time the threats faced by the sector, whether arising from cyber security or other hazards such as extreme weather or aging equipment, are more significant than ever.

Although the regulations have now been in force for 2 years, the security measures in the Government's Code of Practice, which providers are expected to take in order to comply with their new duties, started to fall due in April 2024 and continue until 2028. **Providers are therefore still in the early stages of their security improvement programmes**. We are monitoring their work as they progress.

Our monitoring to date suggests that **industry is taking the threats seriously and progress is being made in securing networks and services**. We actively monitor the 40 largest telecoms providers, together accounting for the vast majority of the revenue and customer services in scope of the security framework. We see early evidence of significant investments underpinning security improvement programmes in most of the providers that we have engaged with, and that these are yielding good progress towards implementations of the first security measures. We do have outstanding questions in relation to some of these measures, such as whether all appropriate measures are being taken to reduce the risks posed by legacy equipment. We are actively engaging with providers to address the highest priority questions.

To ensure providers make the necessary security improvements, we will act when needed. **We have already found compliance breaches with regard to the resilience of a provider's services and have used our enforcement powers.** We imposed a £17.5m penalty on BT due to failures in its emergency communications handling service, which answers 999 calls and routes them to the emergency services. We have an open investigation into a potential breach by Vonage, also relating to emergency calling. Where we consider that providers are falling short of their obligations we will continue to use the enforcement powers the legislation gives us.

During the reporting period we have published detailed new resilience guidance, which sets out the range of measures we expect providers to take in relation to the availability, performance, and functionality of their networks and services under the new security framework.

While it is too early to draw firm conclusions about the effectiveness of the legislation and the security framework it introduced, overall indications are broadly positive. We have no specific policy recommendations at this stage.

[1] Impact Assessment for the Bill - The Telecommunications Security Bill 2020: The Telecoms Security legislation (publishing.service.gov.uk)

Introduction

Following the publication of the findings from the Government's Telecoms Supply Chain Review,[2] on 1 October 2022, the Telecommunications (Security) Act 2021[3] (the 'Security Act') and the associated Electronic Communications (Security Measures) Regulations 2022[4] (the 'Regulations') came into force. Together they place new security duties on providers of public electronic communications networks and services (PECN/S). Ofcom is the regulator responsible for monitoring and enforcing compliance with these duties.

On 1 December 2022, the Telecommunications Security Code of Practice[5] (the 'Code')[6] was published. Made under the Security Act, it provides detailed technical guidance on the measures to be taken by providers under their security duties. The measures in the Code are not binding on providers, however Ofcom is required to take them into account when exercising our relevant functions, as are the courts in any legal proceedings[7].

The Security Act amended the Communications Act 2003 ('the Act') replacing the previous security-related provisions which were contained in sections 105A-D of Act, with new provisions in sections 105A to 105Z29.

Section 105Z of the amended Act requires Ofcom to send a "Security Report" to the Secretary of State after the end of each specified "Reporting Period". The first such Reporting Period was the two years following section 11 of the Security Act entering into force and ended on 1 October 2024. Accordingly, Ofcom has prepared the current document as its first Security Report to the Secretary of State. Subsequent Security Reports will be due annually.

Required contents of this report

Section 105Z provides that:

> "A *security report must contain such information and advice as OFCOM consider may best serve the purpose*" which "*is to assist the Secretary of State in the formulation of policy in relation to the security of public electronic communications networks and public electronic communications services.*"

In particular, section 105Z(4) sets out a number of matters which must be addressed in Security Reports. Table 1 summarises these requirements, and which section(s) and sub-sections of this report addresses each of these.

[2] https://www.gov.uk/government/publications/telecoms-supply-chain-review-terms-of-reference
[3] https://www.legislation.gov.uk/ukpga/2021/31/contents/enacted
[4] https://www.legislation.gov.uk/uksi/2022/933/contents/made
[5] Telecommunications Security Code of Practice
[6] The responsibility for the security framework enacted by the Telecommunications (Security) Act 2021 moved from DCMS to DSIT in February 2023.
[7] Section 105H of the Communications Act 2003.

Table 1: Matters to be included in Security Reports

105Z	Matters to be addressed		Location in this report
(4)(a)	- Extent of compliance with various provisions:		
	s.105A-D	- Duties to take measures	Code monitoring findings
	s.105I	- Explain failure to act in accordance with code of practice	Code monitoring findings/Relevant powers we have not exercised
	s.105J	- Informing users of risk of security compromise	Security compromise reporting/Duty for providers to inform users
	s.105K	- Reporting security compromises to Ofcom	Security compromise reporting
	s.105N(2)(a) & s.105O	- Compliance assessment notices	Code monitoring findings/Relevant powers we have not exercised
(4)(b)	- Extent of acting in accordance with Code		Code monitoring findings
(4)(c)	- Security compromises reported under s105K		Security compromise reporting
(4)(d)	- Ofcom actions in response to s105K reports		Security compromise reporting/ Enforcement activities
(4)(e)	- Extent and manner of Ofcom exercising various functions:		
	s.105I	- Power to notify provider of failure to act in accordance with Code	Code monitoring findings/Relevant powers we have not exercised
	s.105L	- Powers to inform others of security compromise	Security compromise reporting/ Relevant powers we have not exercised
	s.105M	- General duty to ensure compliance	Ofcom's general approach to the Security Act/Code monitoring findings
	s.105N-Q	- Compliance assessment notices	Code monitoring findings/Relevant powers we have not exercised
	s.105S-V	- Enforcement of security duties	Enforcement activities/Exercise of relevant powers & Relevant powers we have not exercised
(4)(f)	- Particular risks to security Ofcom has become aware of		Introduction/General observations on policy matters
(4)(g)	- Other information specified in a direction by the Secretary of State		Introduction/General observations on policy matters

General observations on policy matters

The Security Act established a new security framework which is more detailed than the one it replaced. The framework includes several elements which we detail in this report, in particular the security measures providers should take, requirements to report security compromises, and a range of monitoring and enforcement powers for Ofcom.

We have not yet had cause to use the full range of powers introduced by the Security Act. However, we have successfully taken enforcement action against BT, and currently have no policy concerns in relation to our powers.

The security compromise reporting requirements are generally working well and again we have no policy concerns in relation to them. We do feel that some changes to our existing guidance about our reporting expectations of providers may be beneficial. We discuss these matters in more detail later in this report and explain our intention to consult on revising our guidance accordingly during 2025.

In terms of providers' compliance with the security measures, the framework through the Code explicitly recognises that industry requires time to implement the necessary security measures. This is reflected in the timings associated with the measures in the Code which effectively acknowledge that the required security improvements will take a number of years to complete.

The first measures in the Code fell due on 31 March 2024. This report therefore reflects our observations at a point close to the start of an industry-wide security improvement programme with around four years still to run. Beyond this current work, maintaining compliance with the security duties in light of new threats and technology developments will be an ongoing activity for providers.

Accordingly, we consider it premature to offer observations on the overall effectiveness of the framework in this report. We do however have some policy-related reflections based on our work to date, which are set out in the remainder of this section.

Particular risks of which Ofcom has become aware

Section 105Z(4)(f) requires us to include: *"information about any particular risks to the security of public electronic networks and public electronic communications services of which Ofcom have become aware during the reporting period"*.

Although we became aware of the following risk before the Reporting Period commenced, we highlight it here because our understanding of the risk, and our resultant response, has evolved during the period.

Risk to SS7 signalling from misuse of Global Titles

Global Titles (GTs) enable access to the global mobile signalling network and in the wrong hands they can be misused to try and intercept messages and calls, disrupt the operation of networks and track the location of users of other networks. We found that +44 Global Titles (i.e. those originating from UK telephone numbers, administered by Ofcom) are one of the most significant and persistent sources of malicious signalling traffic affecting mobile networks globally. NCSC is also aware that +44 Global Titles have been exploited for malicious purposes, such as location tracking and the interception of SMS used for 2-step verification (2SV) to target both UK residents and populations globally. Some of this misuse originates from GTs that have been leased to third parties by UK telephone number range holders.

The vulnerabilities of the signalling system exploited by GT misuse are well understood, and mobile operators deploy security measures to address them, including those in the Code. The Code includes defensive measures that providers are expected to take to secure the signalling plane of their networks against external signalling attacks, including those that could be enabled by GT misuse. It also specifies that providers are responsible for the signalling activity and any security implications for GTs that they lease to others. It does not, however, include any technical guidance about measures that operators should take to address the security implications of this, for example to monitor their GT lessees' activities or to prevent their lessees from engaging in malicious signalling activities.

Our provisional view is that the Security Act framework is unlikely to sufficiently address the risk of GT misuse. This is partly because some harmful activities use message types that are also used for legitimate services and cannot therefore be blocked by defensive measures such as firewalls. Also, the Code does not apply to Tier 3 providers and our evidence indicates that some of the lessors we are aware of may be classified as Tier 3.

We consider that a more comprehensive approach that applies to providers of all sizes is needed to address fully the misuse of GTs, and that we can use our number allocation powers to assist in this. Accordingly, in July 2024 we published a consultation[8] which includes proposals to strengthen our existing numbering rules to stop UK mobile number ranges being a source of attacks. We proposed strengthening our rules about the leasing, creation, and misuse of GTs. These measures should significantly reduce the risk of malicious signalling from UK Global Titles, thereby providing material benefits to UK and international citizens. We intend to publish our final decisions on new rules in a Statement in Q4 2024/25.

Other risks

We receive information about relevant risks from a number of sources, such as the security agencies, discussions with the providers we regulate and their suppliers, and publicly available intelligence sources. These risks are generally well understood by the Government's security agencies, and addressed by the measures set out in the Code, for example those posed by the inherent weaknesses in some telecoms signalling protocols. As such, we do not consider these are particular risks which would be relevant to detail in this report.

Another source of information about the risks facing the sector are the causes for incidents which are reported to us under section 105K. The most common causes for resilience-type incidents are typically hardware failures, followed by power cuts. For cyber security incidents, the most common causes are Distributed Denial of Service, ransomware, phishing, and exploitation of published vulnerabilities. All of these risks, which we explore in our Connected Nations reports[9], are generally well understood, and again we do not consider they constitute risks to raise further here.

Telecommunications Security Code of Practice

The Code notes that *"the Government intends to review and update the code of practice periodically as new threats emerge and technologies evolve[10]."* Ofcom's Security Reports are mentioned as one of the sources that will inform such updates.

[8] https://www.ofcom.org.uk/phones-and-broadband/telecoms-infrastructure/consultation-global-titles-and-mobile-network-security/
[9] https://www.ofcom.org.uk/phones-and-broadband/coverage-and-speeds/infrastructure-research/
[10] Paragraph 0.30

We do not consider that there are any new threats or technology evolutions that would warrant updates to the Code at this time. As we work through the existing measures in the Code with providers, we are tracking issues where we consider that revised or additional guidance may be beneficial. Where appropriate, we discuss these matters with The National Cyber Security Centre ("NCSC") and consider whether additional NCSC and/or Ofcom guidance is necessary. We jointly log these issues as items to be considered whenever government next reviews the Code. If we identify any issue which we think may require a more immediate Code update, we will raise this directly with Government.

As noted previously, the final set of measures in the Code fall due at the start of April 2028. Some providers already have significant work programmes underway in order to complete these measures. [redacted] It follows from this that the more the Code itself remains unchanged during this time, the greater the likelihood of maximising the successful delivery of these programmes.

Ofcom's Resilience Guidance

As discussed in more detail in the following section, in September 2024 we published updated network and service resilience guidance for providers, following a consultation.[11] The Security Act defines its central concept – "security compromise" – as including - inter alia - "*anything that compromises the availability, performance or functionality*" of a network or service[12]. Noting that the Code measures mainly relate to minimising the risk of cyber-type security compromises, we considered that our resilience guidance was necessary to set out the range of measures we expect communications providers to take in relation to the availability, performance, and functionality (or 'resilience') of their networks and services. While our guidance is valuable in explaining our expectations to providers, and we will use it as a starting point for considering compliance, it does not have the same standing as codes published by government under section 105E.

Provision of information specified in a direction given by the Secretary of State

Ofcom has not received any directions from the Secretary of State requiring the provision of any additional information during the Reporting Period. Accordingly, we have nothing to report under Section 105Z(4)(g).

[11] Ofcom's Statement on network and service resilience guidance (ofcom.org.uk)
[12] Section 105A(2)(a)

Ofcom's general approach to the Security Act

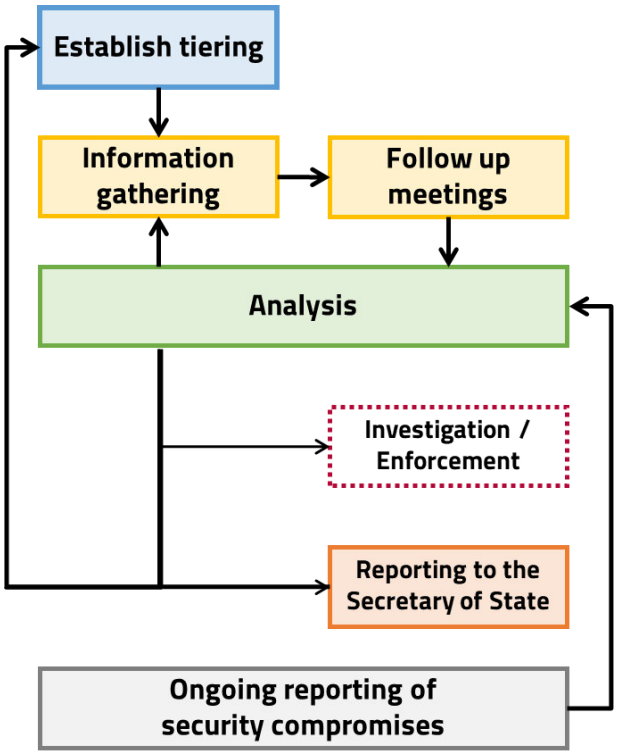
Section overview

- Procedural guidance
- Network and service resilience guidance
- Power resilience in mobile radio access networks
- Other activities

Procedural Guidance

Under section 105Y of the Act, Ofcom has a duty to publish a statement of our general policy with respect to the exercise of our functions under sections 105I and 105M to 105V of the Act. Our procedural guidance, which was published in December 2022[13] following consultation, fulfils this duty and provides general guidance on Ofcom's approach to exercising our functions to seek to ensure compliance with the security duties. In particular, it explains the procedures that we are expecting to follow in carrying out our monitoring and enforcement activity. It also provides guidance about which security compromises we would normally expect providers to report to Ofcom and the process for reporting them, in accordance with section 105K.

Figure 1: Summary of our planned approach to compliance monitoring



[13] General statement of policy under section 105Y of the Communications Act 2003 (ofcom.org.uk)

In Chapter 3 of that document, we set out our planned approach to monitoring providers' compliance with their security duties. This approach is summarised in Figure 1.

Our monitoring work to date, which is explained in more detail in the remainder of this section, has proceeded broadly in accordance with this approach.

We keep our published procedural guidance under review with a view to considering whether any updates are required. We expect to consult on making some updates during 2025. While we do not currently expect to make significant changes to our compliance monitoring approach in this update, we do plan to add references to our recently published resilience guidance (discussed later in this section) and to review our section 105K reporting thresholds and processes.

Network and service resilience guidance

The core security duties introduced by the Security Act are set by reference to the concept of "security compromise", which is defined in section 105A(2) and includes, inter alia: *"anything that compromises the availability, performance or functionality of the network or service"*, and *"anything that causes signals conveyed by means of the network or service to be lost"*.

"Security compromise" therefore includes both "cyber-type" compromises such as those caused by hackers, and other types of impacts on the resilience of PECN/S, such as outages caused by external factors (e.g., floods, cable cuts, or power cuts) or internal factors (e.g., hardware failure, operational process errors, network design flaws).

The Code gives guidance to providers on the measures they should take to ensure compliance with their duties, with these Code measures mainly related to cyber-type security compromises. However, security compromises of any type, not just cyber, can impact the extent to which we can rely on networks and services.

We published our initial resilience guidance under the new framework at the same time as our procedural guidance in 2022, in order to explain our expectations of measures providers should take in relation to non-cyber compromises.[14] During 2023/24 we consulted on and published revised and more extensive network and service resilience guidance[15] which replaced the 2022 resilience guidance. This new guidance applies to the sub-category of security compromises relating to the resilience of networks and services, in terms of availability, performance or functionality ('resilience incidents'). It is intended to be read in conjunction with the Code.

We will use the guidance as a practical reference both:

- in information gathering and monitoring of network and service resilience when engaging with communications providers and the wider industry; and
- as a starting point for considering compliance as part of any enforcement activities in relation to resilience issues.

Power resilience in mobile radio access networks

Alongside our consultation on new resilience guidance, we published a call for input on ensuring power resilience in mobile radio access networks (RAN)[16]. Our aim was to prompt a discussion about

[14] The 2022 guidance replaced resilience guidance relating to the previous framework from 2017.
[15] https://www.ofcom.org.uk/internet-based-services/network-security/resilience-guidance/
[16] Ofcom's Resilience guidance consultation and Call for Input on mobile RAN power back up (ofcom.org.uk)

what power backup mobile network operators can and should provide for their networks and services.

Following the call for input, we set out our next steps on this topic[17]. These included working with operators and the Government to gather additional information about the current power resilience of mobile RAN and assessing the potential costs of meeting resilience expectations. We plan to share our findings from this work with DSIT by the end of this calendar year.

Other activities

Recruitment

The new duties introduced by the Security Act required Ofcom to undertake a significant recruitment campaign to ensure we had sufficient capability and capacity. While the majority of this recruitment related to our technical team, it also impacted other areas such as our legal and enforcement teams. Some concerns about Ofcom's ability to recruit and retain suitable staff were raised during the Parliamentary process for the Security Act. We successfully completed our recruitment activity early in 2024. Ensuring we maintain our capability and capacity in an area of such rapid technical change and skills scarcity remains a challenge and is a constant management focus. However, we do not currently have any particular concerns about our staffing levels, nor do we think it will have any negative impact on our ability to successfully conduct our role in the short term. In the mid to longer term we may need to increase our capacity, for example, in the event we need to do more work on resilience.

Establishing Tiering

The Code divides the providers in scope of the Security Act into three "Tiers", based on their annual relevant turnover. The Code applies differently to providers, depending on the Tier they fall into, and our approach to engagement and compliance monitoring also varies accordingly. Therefore, an important activity for us is to establish which providers fall into which Tiers, and to keep the resultant lists up to date in line with the process set out in the Code.

We have completed our initial assignment of providers to Tiers, based on the annual relevant turnover submissions we receive under our general demand for information for the purposes of calculating administrative charges[18]. We have also completed our first revision, in accordance with the approach set out in the Code[19]. The current number of providers in the Tiers to which the Code applies are as follows:

- **Tier 1** – 7 providers.
- **Tier 2** – 29 providers, 7 of which were added in 2024, due to an increase in their relevant turnover for the preceding 2 years.
- **Tier 3** – the rest of industry; providers in Tier 3 are not expected to follow the measures in the Code[20].

[17] Section 8, Ofcom's Statement on network and service resilience
[18] General demand for information - Ofcom
[19] Paragraph 0.15 of the Code
[20] Paragraph 0.13 of the Code.

Code monitoring

The Code contains detailed guidance for Tier 1 and Tier 2 providers on the measures they should take in order to comply with their security duties. Accordingly, Ofcom's work to monitor compliance is based on developing our understanding of the extent to which these providers are adopting the measures in the Code, and where they are deviating, why and what alternative measures they are taking.

As set out in our procedural guidance, we are primarily doing this using a series of information notices issued under section 135 of the Act. These notices require providers in Tier 1 and Tier 2 to provide details of the security measures they are taking in relation to their PECN/S, with reference to the particular measures set out in the Code. The measures in the Code fall due in groups, starting in April 2024 and continuing until April 2028. The questions in our notices broadly track the groups of measures in the Code as they fall due over this period.

Our first round of information notices was sent to providers in June 2023, and replies were received in early 2024. In this notice we sought to establish the range of the PECN/S that each provider operates, and to gain a high-level understanding of the types of assets they comprise. This allowed us to properly target our later questions and ensure security measures are implemented appropriately across the entirety of each provider's relevant technology estate.

In our first round of notices, we also asked about the measures that had been taken, or were planned, in relation to the first 16 measures in the Code, which fall due in April 2024 or April 2025 (for Tier 1 and Tier 2 providers respectively).

We sent our second round of information notices in June 2024, with responses due in January 2025. These request information about the next 51 measures in the Code, which fall due between April 2024 and April 2025.

Our current findings from this work are discussed in the following section.

Code monitoring findings

As outlined in the previous section of this report, we have started our programme to monitor the adherence of Tier 1 and Tier 2 providers to the Code. This forms a key part of our compliance monitoring activity, and our findings to date are set out in this section.

The section describes the majority of activities relevant to our section 105M duty to seek to ensure providers comply with their security duties.

Section overview

- The purpose of our Code monitoring programme
- Summary of our findings to date
- Summary of themes
- Relevant powers we have not exercised

The purpose of our Code monitoring programme

We have completed our analysis of responses to our first round of information notices. This gives us an understanding, for Tier 1 and Tier 2 providers, of the range of networks, services and assets that are in scope of the duties introduced by the Security Act, and how the providers are going about preparing for the first group of Code measures that fall due.

Particularly for large and long established providers, the activities they need to undertake to implement a given Code measure may impact tens or even hundreds of systems. It is also important to note that responses to our first information notice were due at the beginning of 2024, and none of the Code measures fell due until after this. We are also aware of the regulatory burden that our information gathering activities place on providers. The process is therefore a balance between ensuring that we are fulfilling our functions of overseeing the sector and seeking to ensure compliance, while minimising any unnecessary regulatory burden which might ultimately divert providers' resources away from the core objective of the Security Act which is to improve security.

These considerations mean that our information notice programme is not likely to ever gather a fully comprehensive compliance picture. However, it does allow us to build a baseline understanding of what providers are, or are not, doing in order to meet their security obligations, and to keep this understanding up to date as more of the measures in the Code fall due over the coming years.

The understanding we develop from our Code monitoring is an important input which informs our other engagement with the providers. Other inputs include:

- security compromise reports submitted under section 105K;
- monitoring customer complaints, press reports, and other intelligence sources;
- our work with NCSC, NPSA and others to understand the threats facing the sector and the evolving state of the art in measures to protect against them;
- engagement with the suppliers of equipment and services to the companies we regulate;
- engagement with other UK and international bodies such as regulators and government departments; and
- monitoring of developments in technology and technology standards.

Together these inputs will allow us to target our supervision of providers, using the range of monitoring and enforcement tools and powers available to us.

Summary of our findings to date

- Good engagement with our information notices. For the majority of providers, it is clear they have committed significant resources to answering our questions.
- Evidence of significant investments being underway to improve security in line with the best practices set out in the Code.
- No specific cases of non-compliance have been identified from this first phase of Code monitoring that have caused us to consider it necessary to use our investigation or enforcement powers.
- Generally, providers reported that they were, or were planning to, follow the Code measures rather than pursuing alternative approaches. Accordingly, we have not served any notices under section 105I.
- Generally, providers have good governance practices with established policies, standards and processes in place. In addition, providers are specifically doing well on measures which focus on having security boundaries between the exposed edge and critical functions, ensuring privileged access is regularly reviewed and logged, and changing default passwords when setting up devices or services.

These overall early findings, which relate to the limited number of Code measures addressed in our first information notices, are positive. However, we did have outstanding questions for all providers, raised by their responses. There are several themes that emerge from these questions, which are set out in the following section.

Summary of themes

Scope

- [redacted]
- The UK telecoms industry technical standards body, NICC, has published a guidance document[21] for providers on the interpretation of PECN/S in the context of the Security Act. Both Ofcom and NCSC have raised concerns about the accuracy and utility of this document, and these are captured within the document itself.

Legacy equipment

- Older equipment, some of which may no longer be supported by its manufacturer, is still used by most Tier 1 and some Tier 2 providers. The security challenges this poses are anticipated by the Regulations and the Code[22].
- We see that current approaches and future plans for dealing with the risks from legacy equipment vary, and in some cases we have outstanding questions about whether all appropriate measures will be implemented in good time.

Asset management

- The Code sets out security measures that should be applied to various types of assets, so it is imperative that providers record and track all their assets accurately. [redacted]

[21] https://niccstandards.org.uk/wp-content/uploads/2024/01/ND1448-V1.1.1.pdf
[22] For example, in Regulation 3, and Code measures M4.03 and M4.04.

[redacted]

Signalling weaknesses

- Signalling is the exchange of control information within and between telecoms networks.
- Some providers appear to have weaknesses in relation to some signalling measures which are yet to be addressed. For example, some providers have not explained the technical security measures they have implemented for some of the signalling protocols which we believe they are using. In other cases, the measures that have been described as currently implemented appear to us to be inadequate.

Tier 1 to Tier 2 differences

- Tier 1 providers generally gave higher quality responses, and demonstrated better understanding of security requirements and more security maturity.
- Tier 2 providers' responses were more varied, although this is partly explained by the large diversity caught within Tier 2, in terms of provider scale and scope.

Privileged access workstations (PAWs)

- A privileged access workstation is an appropriately secured device that can be used to administer a network without exposing it to unnecessary threats. This is one of the most important concepts in the Code, with correct implementation of the relevant measures being vital to compliance across a number of Regulations.
- Most of the Code measures relevant to PAWs have not yet fallen due, nor did our first information notice ask about them. Therefore, we do not yet have direct evidence from our monitoring of how providers are addressing privileged access workstations.
- However, our wider engagement with industry, equipment and software vendors, and other agencies, suggests that among many providers this remains one of the most challenging concepts in the Code. We will be monitoring this area particularly closely**.**
- We note that NCSC is working on additional advice to industry related to this topic. We have also engaged with NCSC to support an international standard made available through the European Telecommunications Standards Institute (ETSI)[23], which will support vendors in delivering suitable products to our regulated providers.
- This is another area in which NICC is actively working, although they are yet to publish any resulting guidance or standards. Both Ofcom and NCSC are monitoring this work.

3rd party supplier security

- As with the previous theme, the implementation dates for many of the relevant Code measures have not yet passed. Consequently we currently have limited information on how providers are addressing these measures.
- However, some vendors are telling us that they are seeing widely differing approaches to these measures among their provider customers. Some providers appear to be relying on simple contractual clauses, which may not be sufficiently detailed to deal with the range of measures in the Code. At the other extreme, it appears that some providers might be asking vendors, via contracts, to demonstrate compliance with the full set of security duties.

[23] https://www.etsi.org/deliver/etsi_ts/103900_103999/10399401/01.01.01_60/ts_10399401v010101p.pdf

- We continue to monitor this as the relevant Code measures fall due, via discussions with providers, vendors, and industry bodies. It may be the case that industry will require additional guidance in this area.

Providers acting as suppliers to other providers

- Effectively a special case of the previous theme, we see indications that some service providers, for example mobile virtual network operators (MVNOs), which rely heavily on other network providers as suppliers, may have insufficient security oversight of these arrangements.
- We continue to monitor this as the relevant Code measures fall due.

We are actively engaging with providers to address the highest priority questions raised by our monitoring programme. We are aware of the need for proportionality and to manage the regulatory monitoring burden as we address these questions, not least because our information gathering about the next set of Code measures is underway in parallel.

Relevant powers we have not exercised

During this Reporting Period, we have not exercised our powers under any of the following sections:

- **105I** – directing a provider to explain failure to act in accordance with the Code. Accordingly the extent of provider compliance with section 105I is not applicable.
- **105N, 105O, 105P & 105Q** – issuing assessment notices in order to assess compliance, including urgency statements. Accordingly the extent of provider compliance with section 105N(2)(a) and 105O is not applicable.
- **105O(2)(d)** – power for Ofcom to enter specified premises.

Security compromise reporting

Section overview

- Introduction
- Resilience incidents
- Cyber security incidents
- Dealing with reported incidents
- Duty for providers to inform users
- Relevant powers we have not exercised

Introduction

Section 105K requires providers to notify Ofcom of security compromises that have had, or that enable further compromises that would have, a significant effect on their network or service. As discussed in the "Network and service resilience guidance" section above, security compromises include both resilience incidents and cyber security incidents.

Our procedural guidance provides practical advice in relation to section 105K notifications[24]. This includes when and how providers should submit reports, which varies according to the severity of the incident, and what information we expect to be included. We also set out our views on the types and scale of effect on the operation of a network or service that are likely to be "significant" and therefore indicate that the incident would be notifiable under section 105K.

This section contains summaries of the resilience and cyber incidents that have been reported to us. We also publish additional information about reported incidents, including volume and root cause annual trends, as part of our Connection Nations report. The 2023 edition[25] covers notifications received between September 2022 and August 2023 – the first 11 months of the current Reporting Period. The following 12 months will be included in the 2024 edition, which we expect to publish on our website in December.

Resilience incidents

In terms of volume, the vast majority of the notifications we receive relate to resilience incidents, rather than cyber security incidents. In relation to resilience incidents, the previous reporting duty which was replaced by the Security Act's introduction of section 105K was in effect very similar, and hence this aspect is well established.

One aspect of section 105K which is different to the previous reporting duty is the addition of certain matters to be taken into account in determining whether the effect of an incident is "significant" and hence reportable. Of particular note here are 105K(2)(c) and (d):

[24] Section 5, General statement of policy under section 105Y of the Communications Act 2003.
[25] Connected Nations 2023 - UK report (ofcom.org.uk)

(c) the size and location of the geographical area within which persons who use the network or service are or would be affected by the effect on the operation of the network or service;

(d) the extent to which activities of persons who use the network or service are or would be affected by the effect on the operation of the network or service.

We consider that both of these matters are relevant to networks and services offered in rural areas. The location of users is directly addressed by (c), and with respect to (d), users in more rural areas typically have more limited choices in continuing to conduct their activities in the event of a disruption to their communications services. This may mean that the threshold for the seriousness of an incident that would be reportable may be different where it affects users in rural areas.

Contributing to this view, we have found that resilience incidents in rural areas do sometimes come to our attention, for example through customer complaints, media coverage, and correspondence from MPs, even when they are at scales below our current reporting thresholds.

Another observation from the resilience incidents received during the Reporting Period, is the significant variations in the levels of reporting between different mobile network operators. This may to some extent be due to individual reporting agreements[26] in place with each such provider. These agreements predate the Security Act and were put in place to deal with the difficulties of determining the exact number of end customers affected by incidents in mobile networks.

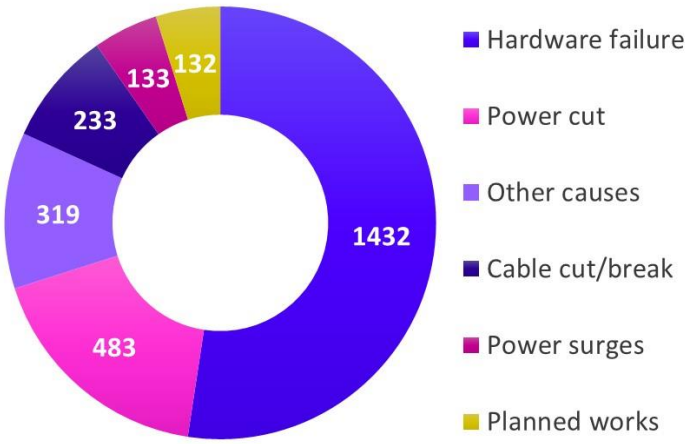
We will consider these matters further and make any changes necessary in order to ensure reporting is as comprehensive as possible, when we next review our current procedural guidance, which we expect to do in 2025.

Summary of resilience incident notifications received during the Reporting Period

- A total of 2732 resilience incidents were reported[27], of which 1510 related to issues affecting fixed networks
- Together the reported incidents resulted in 342 million lost customer hours of normal service availability
- The majority of incidents were attributed to one of two root causes:
    - System failures, for example hardware failures, design errors and faulty network changes, accounting for 2045 incidents
    - 3rd party failures, for example street works causing cable damage, or failed backhaul circuits from wholesale providers, accounting for 632 incidents
- Below these broad categories we also analyse primary causes in more detail, with the most common being:

[26] See Note 5 to Table 2 in General statement of policy under section 105Y of the Communications Act 2003.
[27] All figures for resilience incidents in this section relate to the period from 1 September 2022 to 1 September 2024.

Figure 2: Primary causes of resilience incidents during the Reporting Period



- Changes to networks were the main driver of incidents with the highest customer impacts.
- Extreme weather events commonly result in significant loss of service for customers.
- The number of incidents affecting the PSTN[28] increased by over 50% from the first to the second year of the Reporting Period. We consider this was due, at least in part, to the equipment being beyond its intended lifespan and the decline in qualified personnel within industry with experience of these legacy technologies.

Cyber security incidents

The incident reporting duties introduced by the Security Act are based around "security compromises". The definition of this term is broad and includes incidents that would typically be described as cyber security incidents.

In our 2023 Connected Nations report we noted that we had received a limited number of reported cyber incidents at the time, and that we intended to understand why this was the case[29]. We have since conducted a round of meetings with Tier 1 and some Tier 2 providers to discuss the range of cyber incidents they experience and the processes they have in place to determine which should be reported to Ofcom under section 105K.

From this engagement, it became clear that while cyber security incidents do occur frequently, very few result in significant impacts to the operation of the network or service, and therefore most of them are not reportable. We did not find any indications that providers were failing with respect to their section 105K duty to report cyber incidents.

Outside their section 105K reporting duties, we see some examples of providers sharing findings from their cyber threat intelligence work with us, which suggests an encouraging degree of security maturity is developing in the sector.

[28] Public Switched Telephone Network, the legacy fixed line voice network.
[29] See page 62 of our Connected Nations 2023 main report here: https://www.ofcom.org.uk/siteassets/resources/documents/research-and-data/multi-sector/infrastructure-research/connected-nations-2023/connected-nations-2023-uk-report/?v=330642

Summary of cyber incident notifications received during the Reporting Period

- A total of 15 cyber incidents were reported[30]
- The causes for these incidents fall into several categories, spanning:
    - Distributed Denial of Service (DDoS)
    - Ransomware
    - Phishing
    - Malware
    - Exploitation of vulnerabilities, including zero days
- Of these incidents, four were likely below the thresholds that we consider trigger the mandatory reporting requirement in section 105K.

Pre-positioning attacks

Before the Security Act, only incidents which had already had a significant effect were reportable. However, another important change that was introduced under section 105K(1)(b) is that a security compromise is now reportable if it "*puts any person in a position to be able to bring about a further security compromise that would have a significant effect*". Such events are often referred to as "pre-positioning attacks" – an attacker successfully compromising the security of a system and gaining a foothold within it, such that they could use this to have a significant effect on the operation of a network or service in the future.

These types of security compromises are as likely to indicate an unaddressed security risk in a network or service as an incident which has already had a significant effect. It is therefore equally important that these are reported in order to allow us to assess whether providers have fulfilled their security duties. During our engagement with providers about cyber incident reporting, we did not see specific examples of incidents that providers should have reported under section 105K(1)(b) but failed to do so. However, we did consider that providers were generally less aware of the need to report these sorts of incidents.

It is more difficult to set specific reporting thresholds for cyber incidents than for resilience incidents, because they less often result in a quantifiable service outage. This is especially true for pre-positioning incidents as they rely on a judgement about the potential significance of a subsequent compromise which, by definition, has not actually occurred.

This is another area we will consider carefully when we review our procedural guidance, to determine if we should offer additional guidance to allow providers to reliably identify reportable cyber incidents, including pre-positioning incidents.

Dealing with reported incidents

We use a range of approaches in response to reported incidents, whether resilience or security related. These include:

- Follow up discussions with the affected provider to gain more information about the incident, such as the root cause and contributing factors, the nature and scale of impact, and steps taken before, during and afterwards. This can include obtaining copies of any post incident review reports, and in some cases the use of our information notice powers.

[30] This figure relates to the period from 1 October 2022 to 1 October 2024.

- Logging and categorising reports for use in data analysis, to enable the identification of trends, and to inform our compliance monitoring, our reporting, and the production and updating of industry guidance.
- Additional compliance monitoring, for example where we see inconsistencies between incident reports and other sources of intelligence such as our information gathering programme.
- Structured engagement with a provider, for example to track delivery of compliance improvement plans in the case of repeated and related incidents.
- Use of enforcement powers to investigate a potential compliance breach and impose sanctions where necessary (see Enforcement section for more information).

Duty for providers to inform users

Section 105J requires providers to inform users of their networks and services who may be adversely affected where there is a significant risk of a security compromise occurring. We explain in our procedural guidance that we do not consider providers need to notify users of vulnerabilities which are either unlikely to result in an actual security compromise, or even if they did, they would be unlikely to have an adverse effect on users. We also set out several other factors that providers should take into account when they determine whether and how to inform users.

We are not aware of any instances during the Reporting Period where a provider has informed users in accordance with section 105J. Neither are we aware of any situations in which a provider should have, but failed to do so.

Many providers do provide service status information to their users, often via their websites. These typically report on currently occurring service impacts and planned maintenance events, so are not likely to be directly relevant to section 105J.

Relevant powers we have not exercised

During this Reporting Period, we have not exercised our powers under the following section:

- 105L – informing others of security compromises.

Enforcement activities

Section overview

- Overview of enforcement approach
- Enforcement activity
- Exercise of relevant powers
- Relevant powers we have not exercised

Overview of enforcement approach

The Security Act extended our existing enforcement powers to apply to breaches of the new security duties. We explain our approach to using these powers in our published "Regulatory Enforcement Guidelines for investigations"[31]. We also explain our approach to setting penalties in our published "Penalty guidelines"[32].

We have opened two compliance investigations in relation to potential breaches of the security duties since the Security Act came into force. In one case we concluded the provider, BT, was in breach of its duties in relation to its emergency call handling service, and we imposed a financial penalty. The other investigation into Vonage also relates to emergency calling and is ongoing. Details of both of these cases are published on our website, and summaries are provided below.

Both of these cases resulted from the providers reporting resilience incidents under their section 105K notification duties. No specific compliance concerns which we consider require enforcement action have yet emerged from our Code monitoring work. Nor have we opened a compliance investigation into any of the cyber security incidents reported during the period. However, if we determine there is a potential cyber security related breach of the duties, we will use our enforcement powers accordingly.

Enforcement activity

Compliance investigation CW/01274/06/23 – BT – emergency call services

Summary

We found BT had contravened section 105A(1)(c) of the Act and Regulation 9 of the Regulations by failing to take appropriate and proportionate measures for the purposes of preparing for the occurrence of 'security compromises' in its provision of Emergency Call Handling Services (ECHS).

We imposed a £17.5m penalty[33]. Further details of the case are published on our website[34].

[31] Regulatory Enforcement Guidelines for investigations (ofcom.org.uk)
[32] Penalty guidelines, September 2017 (ofcom.org.uk)
[33] This includes a 30% discount on the penalty figure of £25 million which we would have otherwise imposed. This discount reflects the resource savings achieved by Ofcom as a result of BT's admission of liability and its completion of Ofcom's settlement process.
[34] https://www.ofcom.org.uk/phones-and-broadband/telecoms-infrastructure/bt-999-outage-june-23/

Background

On 25 June 2023, the day the incident occurred, Ofcom received a notification from BT. This explained that BT was experiencing an issue affecting its ability to transfer 999 calls to the Emergency Authorities which resulted in a UK-wide disruption to the ECHS. The incident lasted for a total of 10.5 hours, during which time approximately 23% of all emergency call attempts made were unsuccessful. The severity of the impact varied during the incident; at its worst, 100% of calls to 999 failed during a period lasting 51 minutes.

We issued our confirmation decision under section 96C on 22 July 2024[35]. We have found that BT should have:

a) **ensured it had clearly defined and tested means and procedures** in place for:

i) promptly identifying the occurrence of any security compromise and assessing the severity, impact and likely cause of any security compromise; and

ii) promptly identifying any mitigating actions required as a result of any security compromise; and

b) **put in place an appropriate backup system that had sufficient capacity and functionality** to deal with a level of demand that might reasonably be expected, and had provision for handling emergency Relay calls, which routinely form part of the traffic.

One of the factors we took into account in deciding to impose a penalty in this case, was:

> "providers' compliance with the Security Duties is a priority for Ofcom, and the imposition of a penalty would demonstrate to the wider sector how seriously Ofcom takes compliance with these duties.
>
> Ofcom expects that providers with obligations under the TSA regime – including BT – should invest proactively to meet their Security Duties. As explained in our Penalty Guidelines, we expect management to recognise that it is not more profitable for a business to break the law and pay the consequences than to comply with the law in the first instance."[36]

Compliance investigation CW/01282/03/24 – Vonage – emergency call services

We opened an investigation on 19 March 2024 into Vonage's compliance with sections 105A, 105C and 105K (as well as General Condition A3.2(b)[37]). The opening details are published on our website[38] and any future updates will be available there. The investigation follows Vonage's notification of an incident which resulted in disruption for its business customers to emergency call services between 23 October 2023 and 3 November 2023.

We note that in this case as well as compliance with sections 105A and 105C, which relate to duties to take measures to identify and reduce the risks, prepare for and prevent the adverse effects of security compromises, we are also investigating compliance with section 105K, the duty to inform Ofcom as soon as reasonably practicable of any relevant security compromise.

---

[35] Ofcom's Confirmation decision under section 96C, 22 July 2024 (ofcom.org.uk)
[36] Ofcom's Confirmation decision under section 96C, 22 July 2024 paragraphs 5.9 and 5.10 (ofcom.org.uk)
[37] General conditions of entitlement (ofcom.org.uk)
[38] Investigation into Vonage's compliance with emergency calls access rules (ofcom.org.uk)

Exercise of relevant powers

During this Reporting Period, in undertaking the enforcement activities detailed above, we have exercised our functions under the following sections:

- **96A, 96B, 96C & 97 –** issuing enforcement notices and penalties
- **105S** – which extends our existing enforcement powers in the Act to also apply to breaches of security duties

Relevant powers we have not exercised

During this Reporting Period, we have not exercised our functions under the following sections:

- **98, 99, 100, 102 & 103** - restricting a provider's entitlement to offer electronic communications networks or services, including in urgent cases
- **105T** – which specifies the maximum penalties we can impose in relation to particular types of breach
- **105U & 105V** – proposing and/or directing a provider to take interim steps